The following policy directives and required procedures will be incorporated into ADS 508 within the next few months. In the meantime, please adhere to the policy directives and required procedures contained in this document regarding the roles and responsibilities of the Administrator, the Chief Privacy Officer, and System Owners in the USAID Privacy Program.

Responsibility

Administrator

USAID is charged by law to establish and maintain a federally-compliant Privacy Program. The Administrator must delegate a Chief Privacy Officer (CPO) or other senior level privacy role to have agency-wide oversight and authority for the USAID Privacy Program. USAID must demonstrate that privacy has a high priority within the Agency by implementing an effective privacy management structure and developing a fully integrated privacy program.

The USAID Administrator must:

- Implement a Privacy Program that aligns with Federal law, OMB guidance, and USAID management directives;
- Provide Privacy Awareness training that informs and educates employees and contractors of their responsibilities in protecting privacy information;
- Assign the role of Chief Privacy Officer;
- Identify and report to OMB the senior official(s) primarily responsible to coordinate and implement information technology/Web policies and privacy policies;
- Identify individuals who have day-to-day responsibilities for implementing privacy laws and policy; and
- Designate reviewing officials for USAID privacy impact assessments.

Chief Privacy Officer (CPO)

The USAID Administrator assigned the role of CPO to serve as the principal contact for information technology (IT), Web matters, and privacy policy. The office of the CPO establishes privacy policy and maintains oversight of the USAID Privacy Program. The CPO is also responsible for the following:

- Implementing Agency-wide information privacy protections;
- Sustaining technological privacy protections in the use, collection, sharing, transfer, storage and disclosure of privacy information;
- Maintaining appropriate documentation of privacy information (System of Records Notices, Privacy Impact Assessments, etc.);
- Conducting continuous audits and periodic reviews to identify deficiencies, weaknesses, or risks;
- Enforcing agency-wide privacy policy;
- Establishing education and training on privacy and data protection policies;
- Evaluating legislative and regulatory proposals for collection, use and disclosure of personal information by the Federal Government; and
- Preparing an annual report to Congress detailing Agency activities related to privacy, including complaints of privacy violations, implementation of section 552a of title 5 of United States Code, internal controls, and other relevant matters.

Program oversight includes the following functions:

- Develop and disseminate privacy policies;
- Develop privacy plans and procedures;
- Maintain data quality and protection;
- Arbitrate escalated privacy requests with assistance of General Counsel;

- Oversee annual reporting to OMB on compliance with section 208 of the E-Government Act of 2002;
- Ensure agency compliance with the Paper Reduction Act;
- Promptly, efficiently, and effectively implement policy directives to reduce information collection burdens on the public; and
- Review publications and forms including
    a. Conducting and publishing Privacy Impact Assessments (PIAs),
    b. Creating and publishing System of Records Notices (SORNs),
    c. Creating and submitting Information Collection Requests (ICRs).

System Owners

System Owners for major applications, general support systems, Web sites, databases, or other USAID systems and systems of record, must be knowledgeable about privacy law requirements for such systems. More specifically, as Privacy Act data custodians, they must

a. Verify that systems under their responsibility operate in compliance with USAID privacy policy and Federal privacy laws. This means conducting a privacy impact assessment on every system and filing a System of Record Notice, if applicable.

b. Establish administrative, technical, and physical controls to store and safeguard records from unauthorized access or disclosure, and from physical damage or destruction. System Owners, through the USAID Security Certification and Accreditation (C&A) process, must verify that they have properly implemented the security controls for their information systems, including those that collect, process, store, or transmit personally identifiable information (PII) protected by the Privacy Act. Information about this process is provided in ADS Chapter 545, Information Systems Security.

c. Establish and implement adequate mechanisms to track and report requests filed for privacy information disclosures from systems under his/her responsibility. This requires maintenance of records detailing to whom, what, why, and when PII was disclosed by request, for purposes other than routine USAID business processes. This requirement applies to both manual and automated records. Reports of such requests must be provided to the CPO upon request, but not less than annually for end of fiscal year reporting. System Owners must submit their end of fiscal year reports to the Chief Privacy Officer no later than June 1st of the current fiscal year.